

Written Information Security Program (WISP)

by Melissa J. Krasnow, VLP Law Group LLP, with Practical Law Data Privacy Advisor

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: us.practicallaw.tr.com/w-001-0073

Request a free trial and demonstration at: us.practicallaw.tr.com/about/freetrial

A Standard Document model Written Information Security Program (WISP) addressing the requirements of Massachusetts's Data Security Regulation and the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. It provides general guidance suitable for developing a WISP that other state and federal laws and best practices may require. This Standard Document also includes integrated notes with important explanations and drafting tips.

DRAFTING NOTE: READ THIS BEFORE USING DOCUMENT

A Written Information Security Program (WISP) documents the measures that a business or organization takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains.

This model WISP:

- Addresses the requirements of:
 - Massachusetts's Data Security Regulation (201 Code Mass. Regs. 17.01 to 17.05);
 - similar state laws, such as those of Oregon and Rhode Island (Or. Rev. Stat. § 646A.622; R.I. Gen. Laws § 11-49.3-3(a)(8));
 - the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. §§ 314.1 to 314.5); and
 - state insurance data security laws based on the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668) (for more, see [Practice Note, NAIC Model Data Security Law and State-Specific Implementations](#)).
- Supports an organization's reasonable information security measures that an increasing number of state data security laws require.
- Provides general guidance suitable for developing a WISP that other state and federal laws and best practices may require.

Business Considerations

This Standard Document is a helpful starting point for drafting any WISP, but no model WISP is appropriate for all businesses. In developing a WISP, an organization should consider:

- The size, scope, and type of its business or other activities.
- Its information collection and use practices, including the amount and types of personal or other sensitive information it maintains.
- The need to secure both customer and employee personal information.
- Specific applicable legal requirements, which may depend on, among other things:
 - the nature and industry of the business or organization;
 - the type of information collected and maintained; and
 - the geographic footprint of the business, including the states where the organization's customers and employees reside.
- The resources available to implement and maintain an information security program.



Even when not explicitly required by law, a well-developed and maintained WISP may provide benefits, including:

- Prompting the business to proactively assess risk and implement measures to protect personal and other sensitive information.
- Educating employees and other stakeholders about the actions they need to take to protect personal and other sensitive information.
- Helping to communicate data security expectations and practices to leadership, customers, and other interested parties, such as regulators.
- Establishing that the organization takes reasonable steps to protect personal and other sensitive information, especially if a security incident occurs that risks litigation or enforcement action.

Legal Considerations

This model WISP is helpful in complying with the information security program requirements found in:

- Massachusetts's Data Security Regulation (201 Code Mass. Regs. 17.01 to 17.05) (see Massachusetts Data Security Regulation).
- The GLBA Safeguards Rule (16 C.F.R. §§ 314.1 to 314.5) (see Gramm-Leach-Bliley Act Safeguards Rule).
- Other state laws and best practices with data security requirements (see Drafting Note, Best Practices and Resources and [Practice Notes, State Data Security Laws: Overview](#) and [NAIC Model Data Security Law and State-Specific Implementations](#)).

Massachusetts Data Security Regulation

The Massachusetts Data Security Regulation (201 Code Mass. Regs. 17.01 to 17.05) provides detailed WISP requirements and applies to any business that collects Massachusetts residents' personal information, regardless of business location. This Standard Document follows the Massachusetts Data Security Regulation's requirements and should be used with [Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation](#).

Gramm-Leach-Bliley Act Safeguards Rule

The GLBA applies to financial institutions that collect consumers' non-public personal information (NPI) (16 C.F.R. § 313.3(n)(1)). The GLBA Safeguards Rule requires companies to develop, implement, and maintain a WISP that includes appropriate administrative, technical, and physical safeguards to protect consumer information (16 C.F.R. § 314.3). It also requires them to contractually obligate their service providers who handle NPI to implement and maintain similar safeguards (16 C.F.R. § 314.4(d)).

The Safeguards Rule lays out WISP requirements more broadly than the Massachusetts Data Security Regulation, making this Standard Document also suitable for developing a GLBA-compliant WISP, using alternative language to define personal information (see Drafting Note, Scope: Personal Information). For more details on GLBA and the Safeguards Rule, see [Practice Note, GLBA: The Financial Privacy and Safeguards Rules: The Safeguards Rule](#).

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) applies to certain health care entities and their service providers (business associates). The HIPAA Security Rule requires covered entities and their business associates to:

- Implement and maintain specified administrative, technical, and physical safeguards.
- Implement reasonable and appropriate written policies and procedures.
- Maintain a written record of required activities, such as risk assessments.

(45 C.F.R. §§ 164.302 to 164.318 and see, [Practice Note, HIPAA Security Rule: Safeguards and Related Organizational and Document Requirements](#).)

Covered entities and their business associates should:

- Ensure that their information security policies and procedures are HIPAA-compliant.
- Recognize that a WISP may provide them with a convenient way to organize and describe their information security program.

- Develop and maintain a WISP if required by other applicable laws, such as the Massachusetts Data Security Regulation.

Best Practices and Resources

Several state and federal agencies have issued guidance documents to assist large and small businesses and other organizations in performing risk assessments and developing, implementing, and maintaining their information security programs, including:

- The Federal Trade Commission's (FTC):
 - [Protecting Personal Information: A Guide for Business](#), which provides a five-principle approach to building an information security plan; and
 - [Start with Security: A Guide for Business](#), which offers ten lessons learned from its data security enforcement actions, with practical guidance on how to reduce risks for all businesses.
- The National Institute of Standards and Technology's (NIST) [Framework for Improving Critical Infrastructure Cybersecurity](#), which organizes various globally recognized industry standards and best practices into a model that any organization can adapt and use to identify risks and build an information security program (see [Practice Note, The NIST Cybersecurity Framework](#)).

These resources' recommendations are comparable to the Massachusetts Data Security Regulation's requirements and other similar state and federal laws, while providing additional technical guidance in an accessible form.

Drafting and Implementation Considerations

An organization's WISP should be consistent with its current data collection and information security practices unless specific program plan documentation is in place to close any gaps. Businesses create potential compliance, enforcement, and litigation risks by putting in place and committing to WISPs they do not follow.

Before developing a WISP, an organization should:

- Gather all relevant information regarding the personal and other sensitive information that it

collects, creates, uses, and maintains, including current information security practices.

- Identify all applicable laws and standards that affect the organization's use of personal or other sensitive information, including any contractual obligations.
- Define the WISP's scope, including the personal information, any other sensitive information, and legal requirements it intends to address.

(See Drafting Note, Scope and [Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Preliminary Considerations](#).)

Related Policies and Other Documents

An organization's WISP outlines the purpose, scope, and core elements of its information security program. However, organizations often define their specific security measures in related documents, including:

- Risk assessment reports and remediation plans (for more information on planning and performing risk assessments, see [Practice Note, Data Security Risk Assessments and Reporting](#) and [Performing Data Security Risk Assessments Checklist](#)).
- One or more workforce-facing information security policy documents, such as those that establish policies regarding:
 - information classification and handling practices;
 - user access management and passwords;
 - computer and network security;
 - physical security;
 - incident reporting and response;
 - employee and contractor use of technology, for example, acceptable use and Bring Your Own Device to Work (BYOD) policies; and
 - information systems acquisition, development, and maintenance.

(For more on developing information security policies and an example policy, see [Practice Note, Developing Information Security Policies](#) and [Standard Document, Information Security Policy](#).)

- Process and procedures documents that detail how to implement and maintain particular safeguards, typically for technical or other support staff to use.

Awareness and Training

Organizations should also consider how to best distribute and build awareness of the WISP and related policies, processes, and procedures. For example, businesses may choose to integrate information security training with existing ethics and compliance programs.

At a minimum, organizations should:

- Specifically train all employees and contractors, especially those who handle personal or other sensitive information as part of their duties, on their WISP and relevant policies and procedures (see [Standard Document, Information Security Training: Presentation Materials](#) and [Delivering Information Security Policies and Training Checklist](#)).
- Require all employees and contractors to formally acknowledge their receipt and understanding of the documentation and training, using written forms or an online learning system.
- Retain training and acknowledgment records.

Assumptions

This WISP assumes that the organization only collects, creates, uses, and maintains US residents' personal information. If the organization handles personal information in non-US locations or plans to transfer personal information to the US, it may be subject to data security or privacy laws in those other jurisdictions. Privacy laws vary significantly, and are often more stringent outside the US, especially in the EU (see [Data protection: Country Q&A Tool](#) to compare laws in the US and selected non-US locations).

Bracketed Items

Counsel should complete bracketed items in ALL CAPS with the relevant facts. Bracketed items in sentence case are either optional provisions or include alternative language choices that counsel may select, add, or delete at their discretion.

Written Information Security Program (WISP)

The objectives of this comprehensive written information security program (“**WISP**”) include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards [COMPANY] has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the [Massachusetts Data Security Regulation, 201 Code Mass. Regs. 17.01 to 17.05, other similar US state laws, and [LIST ADDITIONAL APPLICABLE LAWS AND OBLIGATIONS]/LIST SPECIFICALLY APPLICABLE LAWS AND OBLIGATIONS].

If this WISP conflicts with any legal obligation or other [COMPANY] policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

DRAFTING NOTE: WISP OBJECTIVES: APPLICABLE LAWS AND OBLIGATIONS

In this section, the organization should identify the applicable laws, standards, policies, and contractual obligations that may affect its use of personal information or impose obligations on its information

security program (see Drafting Notes, Legal Considerations and Drafting and Implementation Considerations).

Written Information Security Program (WISP)

1. Purpose. The purpose of this WISP is to:
 - (a) Ensure the security, confidentiality, integrity, and availability of personal [and other sensitive] information [COMPANY] collects, creates, uses, and maintains.
 - (b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
 - (c) Protect against unauthorized access to or use of [COMPANY]-maintained personal [and other sensitive] information that could result in substantial harm or inconvenience to any customer or employee.
 - (d) Define an information security program that is appropriate to [COMPANY]'s size, scope, and business, its available resources, and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

DRAFTING NOTE: PURPOSE

This purpose statement tracks the high-level WISP requirements stated in the Massachusetts Data Security Regulation and other similar state and federal laws, including the GLBA (see

[Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Massachusetts Regulation: General WISP Requirements](#)).

2. Scope. This WISP applies to [all employees, contractors, officers, and directors of [COMPANY]/[DEFINE SCOPE]]. It applies to any records that contain personal [or other sensitive] information in any format and on any media, whether in electronic or paper form.
 - (a) For purposes of this WISP, “**personal information**” means either a US resident’s first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:
 - (i) Social Security number;
 - (ii) Driver’s license number, other government-issued identification number, including passport number, or tribal identification number;
 - (iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual’s financial account [GLBA: , or any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information:
 - (A) A consumer provides [COMPANY] to obtain a financial product or service;
 - (B) About a consumer resulting from any transaction involving a financial product or service with [COMPANY];
 - or
 - (C) Information [COMPANY] otherwise obtains about a consumer in connection with providing a financial product or service].
 - (iv) [Health information, including information [regarding the individual’s medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by [COMPANY]]/

Written Information Security Program (WISP)

[HIPAA: , which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual]];

(v) Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;

(vi) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or

(vii) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records.

(c) [

(d) For purposes of this WISP, “**sensitive information**” means data that:

(i) [COMPANY] considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to [COMPANY], its customers, or its business partners.

(iii) Sensitive information includes, but is not limited to, personal information. [See [COMPANY]'s information classification policy, available at [REFERENCE TO POLICY].]

(iv)]

DRAFTING NOTE: SCOPE

The organization should determine whether the WISP applies enterprise-wide or only to selected business units or activities and adjust the scope statement as needed (see [Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Scope of the WISP](#)).

Personal Information

The definition of personal information provided follows the generally applicable Massachusetts Data Security Regulation and similar state laws, such as those of Oregon and Rhode Island (Or. Rev. Stat. § 646A.622; R.I. Gen. Laws § 11-49.3-3(a)(8)). While there are similarities, states often define personal information differently. For details on how each state defines personal information, see [Practice Note, State Data Breach Laws Protected Personal Information Chart: Overview](#).

Generally, the WISP should define personal information considering:

- The data the business collects, creates, uses, or maintains.
- The organization's near-term business plans, such as the states where its customers or employees may reside.
- Applicable laws that the organization references in its privacy policy or other public statements (see [Drafting Note, Legal Considerations](#)).
- What the organization otherwise considers personal information, including any information that it must protect by contract with third parties.

If applicable:

- Section 2(a)(iii) should include the additional text to meet GLBA's definition of non-public personal information (16 C.F.R. § 313.3(n)(1)).

- Section 2(a)(iv) should use the optional text regarding HIPAA to meet HIPAA's requirements (45 C.F.R. § 160.103).

Sensitive Information

If the organization intends for the WISP to cover other data that it considers to be sensitive, in addition to personal information, then counsel should include the optional text in this section and throughout the WISP. For example, a business may wish to apply the same WISP to highly confidential information regarding its products, business plans, or certain operations (or third-party contracts may require it to do so).

Sensitive or highly confidential information:

- Typically includes data that if accessed by or disclosed to unauthorized parties could cause **significant or material harm** to the organization, its customers, or its business partners.
- Includes, but is not limited to, personal information.
- Contrasts with an organization's less sensitive, but still non-public internal use only or confidential information.

If the organization has an information classification policy, for example, as part of its information security policies and procedures (see Section 5), the WISP should include a reference as shown in the optional text.

3. Information Security Coordinator. [COMPANY] has designated [TITLE] to implement, coordinate, and maintain this WISP (the "**Information Security Coordinator**"). The Information Security Coordinator shall be responsible for:

- (a) Initial implementation of this WISP, including:
- (i) Assessing internal and external risks to personal [and other sensitive] information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);
 - (ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);
 - (iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal [and other sensitive] information (see Section 6);
 - (iv) Ensuring that the safeguards are implemented and maintained to protect personal [and other sensitive] information throughout [COMPANY], where applicable (see Section 6);
 - (v) Overseeing service providers that access or maintain personal [and other sensitive] information on behalf of [COMPANY] (see Section 7);
 - (vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);
 - (vii) Defining and managing incident response procedures (see Section 9); and
 - (viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with [COMPANY] human resources and management (see Section 10).
- (b) Employee, contractor, and (as applicable) stakeholder training, including:
- (i) Providing periodic training regarding this WISP, [COMPANY]'s safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal [or other sensitive] information;
 - (ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through [written acknowledgement forms/[DESCRIBE ANY ONLINE ACKNOWLEDGMENT PROCESS]]; and
 - (iii) Retaining training and acknowledgment records.

Written Information Security Program (WISP)

- (c) Reviewing this WISP and the security measures defined here at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information (see Section 11).
- (d) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or [COMPANY]'s information security policies and procedures.
- (e) Periodically reporting to [COMPANY] management regarding the status of the information security program and [COMPANY]'s safeguards to protect personal [and other sensitive] information.

DRAFTING NOTE: INFORMATION SECURITY COORDINATOR

Considerations for designating an information security coordinator depend on the organization's specific circumstances and may include:

- The organization's size, industry, and regulators.
- The types of personal and other sensitive information the organization owns or maintains on behalf of others.
- The employees responsible for the organization's compliance with security requirements, including compliance with its internal policies and procedures, contracts, and relevant laws and industry standards.
- Leadership support and sponsorship to ensure the information security coordinator has sufficient authority to implement and enforce the WISP.

The organization should also consider the appropriate business units to involve in program oversight, which may include:

- Legal.
- Information technology (IT).
- Privacy or a broader ethics and compliance unit.

The specific title used for the information security coordinator role may also vary according to the organization's size, industry, and other characteristics. Counsel should draft the WISP to refer to the coordinator by current title, and not individual name, to minimize maintenance requirements and any potential confusion if personnel change.

4. Risk Assessment. As a part of developing and implementing this WISP, [COMPANY] will conduct a periodic, documented risk assessment[, at least annually, or whenever there is a material change in [COMPANY]'s business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information].

- (a) The risk assessment shall:
 - (i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal [or other sensitive] information;
 - (ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal [and other sensitive] information; and
 - (iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
 - (A) Employee, contractor, and (as applicable) stakeholder training and management;
 - (B) Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

Written Information Security Program (WISP)

- (C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
- (D) [COMPANY]'s ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.
- (b) Following each risk assessment, [COMPANY] will:
- (i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
 - (ii) Reasonably and appropriately address any identified gaps; and
 - (iii) Regularly monitor the effectiveness of [COMPANY]'s safeguards, as specified in this WISP (see Section 8).

DRAFTING NOTE: RISK ASSESSMENT

Risk assessment is a critical element of any information security program. Information security risks are best understood using this simple equation: **risk = threat + vulnerability**.

Threats may include external bad actors or internal (employee or contractor) lapses, whether inadvertent or intentional. Vulnerabilities cover a wide range of issues related to process, people, and technology, such as:

- Untrained or inattentive individuals.
- Improperly secured facilities.
- Poor implementation, configuration, or maintenance practices.
- Flaws in network and computer assets, including hardware, software, and application issues.

See Drafting Note, Best Practices and Resources and [Practice Notes, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation: Identifying and Minimizing Reasonably Foreseeable Internal and External Risks](#)

and [Data Security Risk Assessments and Reporting](#) for guidance on risk assessments.

Risks change over time as:

- Novel threats emerge.
- Vulnerabilities are identified and become widely known.
- The business evolves, especially when it:
 - makes changes in data collection and handling practices;
 - introduces new or materially changed products and services;
 - alters its business processes and practices; or
 - deploys new, or updates existing, network and computer environments.

Organizations should develop processes to assess risks on an ongoing basis and periodically update their formal risk assessment. These updates should occur at least annually or whenever there is a material change in applicable business practices.

5. [Information Security Policies and Procedures](#). As part of this WISP, [COMPANY] will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

- (a) Establish policies regarding:
- (i) Information classification;
 - (ii) Information handling practices for personal [and other sensitive] information, including the storage, access, disposal, and external transfer or transportation of personal [and other sensitive] information;

Written Information Security Program (WISP)

- (iii) User access management, including identification and authentication (using passwords or other appropriate means);
 - (iv) Encryption;
 - (v) Computer and network security;
 - (vi) Physical security;
 - (vii) Incident reporting and response;
 - (viii) Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and
 - (ix) Information systems acquisition, development, operations, and maintenance.
- (b) Detail the implementation and maintenance of [COMPANY]'s administrative, technical, and physical safeguards (see Section 6).

DRAFTING NOTE: INFORMATION SECURITY POLICIES AND PROCEDURES

Information security policies:

- Serve as a foundational administrative safeguard by providing clear guidance and limits for employees, contractors, and other stakeholders.
- Explain how the organization classifies various forms of data, which in turn defines the level and nature of required safeguards.
- Should be written for and accessible to all employees, contractors, and other stakeholders.

- Should be periodically reviewed and updated as risks and the business change.

Information security procedures:

- Document how the organization implements and maintains its selected safeguards.
- Often include technical details intended primarily for IT or other support staff.

6. **Safeguards.** [COMPANY] will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal [or other sensitive] information that [COMPANY] owns or maintains on behalf of others.

- (a) Safeguards shall be appropriate to [COMPANY]'s size, scope, and business, its available resources, and the amount of personal [and other sensitive] information that [COMPANY] owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.
- (b) [COMPANY] shall document its administrative, technical, and physical safeguards in [COMPANY]'s information security policies and procedures (see Section 5).
- (c) [COMPANY]'s administrative safeguards shall include, at a minimum:
 - (i) Designating one or more employees to coordinate the information security program (see Section 3);
 - (ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 4);
 - (iii) Training employees in security program practices and procedures, with management oversight (see Section 3);

Written Information Security Program (WISP)

- (iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7); and
 - (v) Adjusting the information security program in light of business changes or new circumstances (see Section 11).
- (d) [COMPANY]'s technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:
- (i) Secure user authentication protocols, including:
 - (A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;
 - (B) Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
 - (C) Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
 - (ii) Secure access control measures, including:
 - (A) Restricting access to records and files containing personal [or other sensitive] information to those with a need to know to perform their duties; and
 - (B) Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.
 - (iii) Encryption of all personal [or other sensitive] information traveling wirelessly or across public networks;
 - (iv) Encryption of all personal [or other sensitive] information stored on laptops or other portable or mobile devices [, and to the extent technically feasible, personal [or other sensitive] information stored on any other device or media (data-at-rest)];
 - (v) Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal [or other sensitive] information or other attacks or system failures;
 - (vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal [or other sensitive] information; and
 - (vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.
- (e) [Company]'s physical safeguards shall, at a minimum, provide for:
- (i) Defining and implementing reasonable physical security measures to protect areas where personal [or other sensitive] information may be accessed, including reasonably restricting physical access and storing records containing personal [or other sensitive] information in locked facilities, areas, or containers;
 - (ii) Preventing, detecting, and responding to intrusions or unauthorized access to personal [or other sensitive] information, including during or after data collection, transportation, or disposal; and
 - (iii) Secure disposal or destruction of personal [or other sensitive] information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

DRAFTING NOTE: SAFEGUARDS

The safeguards detailed here track the Massachusetts Data Security Regulation and other similar state laws, including Oregon's statute, as well as the GLBA Safeguards Rule. Organizations that are subject to HIPAA should update the administrative, technical, and physical safeguards accordingly (see [Practice Note, HIPAA Security Rule](#)).

Organizations should not only examine applicable laws but also determine the feasibility of implementing and maintaining safeguards in their environments. According to [guidance](#) from the Massachusetts Office of Consumer Affairs and Business Regulation, "technically feasible" means that if there is a reasonable means through technology to accomplish a required result, the organization must use such reasonable means.

Legal requirements generally call for encrypting personal information when storing it on mobile devices or transmitting it wirelessly or over public networks. However, to better manage risk, organizations may choose to expand their encryption programs to include any stored personal information (data-at-rest) to the extent feasible, as shown in the optional text. For example, many federal and

state data breach notification laws provide safe harbor from notice requirements when organizations encrypt personal data and a cyber incident does not compromise the encryption keys or other similar controls.

Organizations that implement additional safeguards and related processes, such as those addressing bug bounty and vulnerability disclosure, should consider:

- Describing those program elements in their WISPs to provide a comprehensive view of their information security capabilities.
- Referencing their more detailed process and technical documents, as applicable.

For more on these programs, see [Practice Note, Bug Bounty and Vulnerability Disclosure Programs](#) and [Building a Bug Bounty and Vulnerability Disclosure Program Checklist](#).

To minimize potential compliance risk and liability, organizations should meet the safeguards commitments they make in their WISPs or have a reasonable, documented remediation plan in place to close any gaps.

7. Service Provider Oversight. [COMPANY] will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal [or other sensitive] information on its behalf by:

- (a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.
- (b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and [COMPANY]'s obligations.
- (c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and [COMPANY]'s obligations.

DRAFTING NOTE: SERVICE PROVIDER OVERSIGHT

Organizations should:

- Conduct data security due diligence on their service providers before engagement and monitor and audit

ongoing performance (for an example form, see [Standard Document, Vendor Due Diligence: Security and Privacy Questionnaire](#)).

Written Information Security Program (WISP)

- Identify their applicable existing service providers and, if necessary, amend their contracts to ensure compliance with applicable laws and the WISP.
- Include specific requirements in new service provider agreements involving personal or other sensitive information to address compliance with applicable laws and the WISP.

- Address service provider oversight in employee training.

For more details on developing a service provider oversight program, see [Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships](#).

8. **Monitoring.** [COMPANY] will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal [or other sensitive] information. [COMPANY] shall reasonably and appropriately address any identified gaps.

9. **Incident Response.** [COMPANY] will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

- (a) Documenting the response to any security incident or event that involves a breach of security.
- (b) Performing a post-incident review of events and actions taken.
- (c) Reasonably and appropriately addressing any identified gaps.

DRAFTING NOTE: INCIDENT RESPONSE

Organizations should develop and test cyber incident response plans (IRPs) that address how they prepare for and handle cyberattacks, data breaches, and other information security incidents. An organization's IRP should set out each step to take once the organization detects a potential security incident. The IRP should comply with

the organization's legal obligations and reflect its operational realities. For a checklist outlining key steps to take when developing an IRP, see [Developing a Cyber Incident Response Plan Checklist](#). For a model IRP with integrated guidance and drafting tips, see [Standard Document, Cyber Incident Response Plan \(IRP\)](#).

10. **Enforcement.** Violations of this WISP will result in disciplinary action, in accordance with [COMPANY]'s information security policies and procedures and human resources policies. Please see [REFERENCE TO HR POLICIES] for details regarding [COMPANY]'s disciplinary process.

DRAFTING NOTE: ENFORCEMENT

Organizations must impose disciplinary measures for WISP violations under the Massachusetts Data Security Regulation. Other laws may require similar sanctions. To avoid employee confusion and potential conflicts, rather than creating its own disciplinary

process, the WISP should refer to established human resources policies and processes. Information security policies and procedures may further define prohibited actions and compliance processes.

Written Information Security Program (WISP)

11. Program Review. [COMPANY] will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in [COMPANY]'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

(a) [COMPANY] shall retain documentation regarding any such program review, including any identified gaps and action plans.

DRAFTING NOTE: PROGRAM REVIEW

The Massachusetts Data Security Regulation and best practices require that a business review its WISP on at least an annual basis or whenever there is a material

change in business practices that may implicate the security or integrity of records that contain personal (or other sensitive) information.

12. Effective Date. This WISP is effective as of [DATE].

(a) Revision History: [Original publication/[NOTE SUBSEQUENT REVISIONS]].

DRAFTING NOTE: EFFECTIVE DATE

The WISP should include an effective date and identify any subsequent revisions. The organization should briefly note in the revision history any material updates and their drivers, such as a periodic program

review or change in business processes, laws, or identified risks. The organization should retain prior versions of the WISP to demonstrate the program that was in effect at any particular time.

About Practical Law

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.